REMARKS

The application has been amended and is believed to be in condition for allowance.

Claim 5 has been amended responsive to the noted informality.

The title was said not to be descriptive of the invention as claimed. The title has been amended to "DNS SERVER FILTER CHECKING FOR ABNORMAL DNS PACKETS". Should this title not be acceptable, applicant respectfully requests an acceptable title be suggested.

The previously pending claims have been amended.

New claims 19-20 depend from claims 7 and 13 respectively and recite features of the invention discussed below.

Claims 1-13 were rejected as anticipated by DONALDSON et al. 6,321,267 ("DONALDSON"). The claims, as amended, are believed patentable. Reconsideration and allowance of all the pending claims are respectfully requested.

The DNS server filter of the present invention checks (filters) for an abnormality of a DNS packet both moving i) from the inside network to the outside network (the network inside the organization to the network outside the organization), and ii) from the outside network to the inside network. See specification page 34, line 8 through page 35, line 6.

In this way, the invention prevents a packet having an abnormal format from being sent both into an organization's DNS server and out from an organization's network into outside DNS servers. Accordingly, each DNS server, in both the inside network and the outside network, can be kept in normal operation, free of abnormal format packets.

Consider the recitations of dependent new claims 19-20 reciting features respecting filtering of both incoming and outgoing DNS packets.

See that the invention provides that the incoming DNS packet is checked for the any abnormality by obtaining information on a host name, a domain name, and an IP (Internet protocol) address transmitted from the network outside an organization by a person outside the organization using a DNS protocol, and, that detection of the any abnormality prevents the incoming DNS packet from being transmitted into the organization's network. Thus, the person outside the organization is prevented from invading a network of the organization by using private information of the organization and preventing the DNS server from operating abnormally by receiving a packet having an abnormal format.

Additionally, the claims recite that the invention provides that the outgoing DNS packet is also checked for the any abnormality by obtaining information on a host name, a domain name, and an IP address transmitted to a DNS server belonging to

a network outside the organization by a person inside the organization using a DNS protocol, and, the that detection of the any abnormality prevents the outgoing DNS packet from being transmitted outside the organization's network. Thus, the person inside the organization is likewise prevented from invading the network outside the organization.

In contrast, DONALDSON discloses a technique concerned with mail filtering in the SMTP. DONALDSON does not disclose DNS packet filtering as recited. In DONALDSON, the DNS is simply mentioned to get the IP address of the destination host or the IP address from an MX record for the domain (see column 2, lines 48-62).

Further, to the extent that DONALDSON might be viewed as a DNS filter, DONALDSON only checks electronic junk mail received at a MTA (i.e., an inside network) from remote Internet hosts using the SMTP (i.e., an outside network). DONALDSON never checks (filters) mails sent from the inside network to the outside network, and cannot prevent faulty packets from being sent to DNS servers in the outside network.

Thus, DONALDSON fails to anticipate.

Amended claim 1 is not anticipated as there is no disclosure of packet verification means for verifying whether there is any abnormality in contents of a received (incoming) DNS packet before transmitting it to a DNS server and for verifying whether there is any abnormality in contents of a to-be-

transmitted DNS packet (outgoing) before transmitting it outside the network.

As to independent claim 7, see the recitations of receiving an inquiry from both

i) within inside an organization's network, concerning an outgoing DNS packet, and ii) from outside an organization's network, concerning an incoming DNS packet,

so as to provide packet verification for verifying whether there is any abnormality in contents of the incoming DNS packet before transmitting the packet to the inside the organization's network and for verifying whether there is any abnormality in contents of the outgoing DNS packet before transmission from inside the organization's network to outside the organization's network.

These recitations are not anticipated.

Similar reasoning applies to independent claims 13 and 17.

The dependent claims are believed allowable at least for depending from an allowable independent claim. However, the substantively amended claims are also believed patentably in their own right.

Further, as to the recitations of original claim 3, the Official Action indicates the DONALDSON column 17, lines 36-67 and column 18, lines 1-31 are anticipatory.

These passages are not believed to anticipate, and attention is directed to the disclosure beginning at line 20 of column 14, which discloses explains the operation of the DONALSON filter. The relevant passage is reproduced below (emphasis added):

> Operation
>
> FIG. 13 provides an overview of the present invention, with more detailed operation shown in FIGS. 14-23. The figure shows the key steps used by the Active Filter Proxy 1401 to validate a single email message from a remote host 1400 and transfer the message to the protected MTA 1402. A separate SMTP connection 1418 is used for actively probing the remote host in order to perform Active Dialup 1420 detection and Active Relay 1450 detection. An additional connection may be established to a different mailhost for Active User testing. The Active Filter Proxy 1401 corresponds to proxy 1104 shown in FIG. 7.
>
> The proxy 1401 is shown in FIG. 13 connected between the remote host 1400 and the local MTA 1402. The proxy 1401 and MTA 1402 may be located at separate hosts, as shown in FIGS. 8 and 12, or at a same host as shown in FIGS. 9-11. Because the proxy 1401 controls when it reads data on the connection 1403, it is not possible for the remote host 1400 to proceed with transfer of its message until the proxy 1401 completes its filtering. *The proxy only handles incoming email and does not process outgoing email from the MTA to remote hosts. Outgoing email is sent directly from the MTA 1402 to the network.*

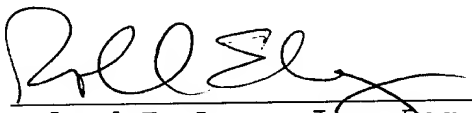
In view of the above, reconsideration and allowance of all the claims are respectfully requested.

Applicant believes that the present application is in condition for allowance and an early indication of the same is respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/fb